On generic erasure correcting sets and related problems

R. Ahlswede and H. Aydinian*
Department of Mathematics
University of Bielefeld
POB 100131,
D-33501 Bielefeld, Germany
ahlswede@math.uni-bielefeld.de
ayd@math.uni-bielefeld.de

***Abstract*— Motivated by iterative decoding techniques for the binary erasure channel Hollmann and Tolhuizen introduced and studied the notion of generic erasure correcting sets for linear codes. A generic (r, s)–erasure correcting set generates for all codes of codimension r a parity check matrix that allows iterative decoding of all correctable erasure patterns of size s or less. The problem is to derive bounds on the minimum size $F(r, s)$ of generic erasure correcting sets and to find constructions for such sets. In this paper we continue the study of these sets. We derive better lower and upper bounds. Hollmann and Tolhuizen also introduced the stronger notion of (r, s)–sets and derived bounds for there minimum size $G(r, s)$. Here also we improve these bounds. We observe that these two conceps are closely related to intersecting codes, an area, in which $G(r, s)$ has been studied primarily with respect to ratewise performance. We derive connections. Finally, we observed that hypergraph covering can be used for both problems to derive good upper bounds.**

I. INTRODUCTION

Iterative decoding techniques, especially when applied to low-density parity-check codes, have recently attracted a lot of attention. It is known that the performance of iterative decoding algorithms in case of a binary erasure channel depends on the sizes of the *stopping sets* associated with a collection of parity check equations of the code [11]. Let H be a parity–check matrix of a code $\mathcal{C}$, defined as a matrix whose rows span the dual code $\mathcal{C}^{\perp}$. A stopping set is a nonempty set of code coordinates such that the submatrix formed by the corresponding columns of H does not contain a row of weight one. Given a parity-check matrix H, the size of the smallest nonempty stopping set, denoted by $s(H)$, is called the *stopping distance* [27] of the code with respect to H. Iterative decoding techniques, given a parity check matrix H, allow to correct all erasure patterns of size $s(H)$ or less. Therefore, for better performance of iterative erasure decoding it is desired that $s(H)$ be as large as possible. Since the support of any codeword (the set of its nonzero coordinates) is a stopping set, we have $s(H) \leq d(\mathcal{C})$ for all choices of H. It is well known that the equality can always be achieved, by choosing sufficiently many vectors from the dual code $\mathcal{C}^{\perp}$ as rows in H. This motivated Schwartz and Vardy [27] to introduce the notion of *stopping redundancy* of a code. The stopping redundancy of $\mathcal{C}$, denoted by $\rho(\mathcal{C})$, is the minimum number of rows in a parity-check matrix such that $s(\mathcal{C}) = d(\mathcal{C})$.

Schwartz and Vardy [27] derived general upper and lower bounds, as well as more specific bounds for Reed–Muller codes, Golay codes, and MDS codes. Improvements upon general upper bounds are presented in [13], [14]. The stopping redundancy of Reed–Muller codes was further studied by Etzion [12]. Hehn et al. [15] studied the stopping redundancy of cyclic codes.
Recall that a binary linear code $\mathcal{C}$ is capable of correcting those and only those erasure patterns that do not contain the support of a non-zero codeword. These patterns are called *correctable* for $\mathcal{C}$. All other erasure patterns are called *uncorrectable*. Note that the size of a correctable erasure pattern for a code can be greater than its minimum distance and it is upper bounded by the codimension of the code.

Hollmann and Tolhuizen [17] observed that given a linear code $\mathcal{C}$, any correctable erasure pattern can be iteratively decoded provided a chosen parity check matrix contains sufficiently many rows. This motivated them [17] to introduce the notion of *generic erasure correcting sets* for binary linear codes. A generic (r, s)–erasure correcting set, *generic* (r, s)*–set* for short, generates for all codes of codimension r a parity check matrix that allows iterative decoding of all correctable erasure patterns of size s or less. More formally, a subset $\mathcal{A}$ of a

This author was supported by the DFG Project AH46/8-1

binary vector space $\mathbb{F}_2^r$ is called generic (r,s)–set if for any binary linear code $\mathcal{C}$ of length n and codimension r, and any parity check $r \times n$ matrix H of $\mathcal{C}$, the set of parity check equations $\mathcal{H}_{\mathcal{A}} = \{\mathbf{a}H : \mathbf{a} \in \mathcal{A}\}$ enables iterative decoding of all correctable erasure patterns of size s or less.

Weber and Abdel–Ghaffar [30] constructed parity check matrices for the Hamming code that enable iterative decoding of all correctable erasure patterns of size at most three. Hollmann and Tolhuizen [16] [17] gave a general construction. They also established upper and lower bounds for the minimum size of generic (r,s)–sets.

Throughout the paper we use the following notation. We use $[n,k,d]_q$ for a linear code $\mathcal{C}$ (of length n, dimension k, and minimum Hamming distance d) over $\mathbb{F}_q$. The Hamminng weight of a vector $\mathbf{a}$ is denoted by $wt(\mathbf{a})$. We denote by $[n]$ the set of integers $\{1,\dots,n\}$. A k–element subset of a given set is called for short a k–subset. $\mathbb{F}_q^{k\times m}$ denotes the set of all $k \times m$ matrices over the finite field $\mathbb{F}_q$. For integers $0 \le k \le m$, $\left[{m \atop k}\right]_q$ stands for the q-ary Gaussian coefficient, defined by $\left[{m \atop 0}\right]_q = 1$ and $\left[{m \atop k}\right]_q = \prod_{i=0}^{k-1} \dfrac{(q^{m-i}-1)}{(q^{k-i}-1)}$ for $k = 1,\dots,m$. It is well known that $\left[{m \atop k}\right]_q$ is the number of k–dimensional subspaces in $\mathbb{F}_q^m$. A k–dimensional subspace is called for short a k–subspace. A coset of a k–subspace in $\mathbb{F}_q^m$ is called a k–dimensional plane or shortly k–plain. Recall that there are $q^{m-k}\left[{m \atop k}\right]_q$ k–plains in $\mathbb{F}_q^m$. A k–plain which is not a subspace is called a k–flat. Later on we will omit q in the notation above for the binary case.

In this paper we continue the study of generic erasure correcting sets. Let $F(r,s)$ denote the minimum size of a generic (r,s)–set. The bounds for $F(r,s)$ presented below are due to Hollmann and Tolhuizen. The following is the best know constructive bound

Theorem 1: [17] For $2 \le s \le r$ we have

$$F(r,s) \le \sum_{i=1}^{s-1} \binom{r-1}{i}. \tag{I.1}$$

It is clear that any upper bound for $F(n-k,d-1)$ is an upper bound for the stopping distance $\rho(\mathcal{C})$ of an $[n,k,d]$ code, thus $\rho(\mathcal{C}) \le F(n-k,d-1)$ Therefore, for an $[n,k,d]$ code $\mathcal{C}$ one has the bound

$$\rho(\mathcal{C}) \le F(n-k,d-1) \le \sum_{i=1}^{d-2} \binom{n-k-1}{i}, \tag{I.2}$$

which turns to be also the best constructive bound for the stopping redundancy.

We notice that the best known nonconstructive upper bounds for the stopping redundancy of a linear code are given in Han and Siegel [13] and in Han et al [14].

Theorem 2: [13] For an $[n,k,d]$ code $\mathcal{C}$ with $r = n-k$ we have

$$\rho(\mathcal{C}) \le \min\{t \in \mathbb{N} : \sum_{i=1}^{d-1} \binom{n}{i} \Big(1 - \frac{i}{2^i}\Big)^t < 1\} + r - d + 1. \tag{I.3}$$

A closed form expression derived from this bound is as follows

Corollary 1: For an $[n,k,d]$ code $\mathcal{C}$ with $r = n-k$ we have

$$\rho(\mathcal{C}) \le \frac{\log \sum_{i=1}^{d-1} \binom{n}{i}}{-\log\Big(1 - \frac{d-1}{2^{d-1}}\Big)} + r - d + 1. \tag{I.4}$$

(where $\log$ is always of base 2). Further improvements upon the probabilistic upper bound are given in [14].

There is a big gap between the lower and upper bounds for $F(r,s)$.

Theorem 3: [16] For $1 \le s \le r$ the following holds

$$r \le F(r,s) \le \frac{rs}{-\log(1-\frac{s}{2^s})}. \tag{I.5}$$

The upper bound is derived by a probabilistic approach.

In [16] introduced and studied a related notion of (r,s)-good set. A subset $\mathcal{A} \subseteq \mathbb{F}^r$ is called (r,s)-1 good if for any s linearly independent vectors $\mathbf{v_1},\dots,\mathbf{v_s} \in \mathbb{F}_2^r$ there exists a $\mathbf{c} \in \mathcal{A}$ such that the inner product $(\mathbf{c},\mathbf{v_j}) = 1$ for $j = 1,\dots,s$. $\mathcal{A}$ is called (r,s)-good if for any linearly independent vectors $\mathbf{v_1},\dots,\mathbf{v_s} \in \mathbb{F}_2^r$ and for arbitrary $(x_1,\dots,x_s) \in \{0,1\}^s$ there exists $\mathbf{c} \in \mathcal{A}$ such that $(\mathbf{c},\mathbf{v_j}) = x_j$ for $j = 1,\dots,s$.

We denote by $G_1(k,s)$ the minimum cardinality $|\mathcal{A}|$ for which there exists a (k,s)-1 good set $\mathcal{A}$. The corresponding notation for (r,s)–good sets is $G(r,s)$. Hollman and Tolhuizen [16] observed that adding the zero vector to an (r,s)-1 good set we get an (r,s)–good set and $G_1(r,s) = G(r,s) - 1$. So these two notions are essentially the same.

Later on we consider only (r,s)-1 good sets and call them for short just (r,s)–sets. Obviously every (r,s)–set is a generic (r,s)–set, thus $G_1(r,s) \ge F(r,s)$.

Theorem 4: [16]. For $1 \le s \le r$ the following holds

$$2^{s-1}(r-s+2)-1 \le G_1(r,s) \le \frac{rs - \log s!}{-\log(1-2^{-s})}. \tag{I.6}$$

The upper bound is obtained again by a probabilistic argument.

The paper is organized as follows.

In Section 2 we obtain some properties of generic (r,s)–erasure correcting sets and (r,s)–sets which we use later. In Section 3 we show that the problem we study here is closely related to s–wise intersecting codes studied in

the literature.
In Section 4 we focus on bounds for $F(r,s)$ and $G_1(r,s)$. We improve the bounds (1.5) and (1.6) in Theorems 11–15. In particular, we show that for $2 \leq s < r$ we have

$$3 \cdot 2^{s-2}(r-s) + 5 \cdot 2^{s-2} - 2 \leq G_1(r,s) \leq \frac{(r-s+1)s+2}{-\log(1-2^{-s})},$$

$$F(r,s) > \max\{2^{s-1}+r-s, G_1(k-\lceil s/2 \rceil, \lfloor s/2 \rfloor)\},$$

$$F(r,s) < \frac{rs - \log s!}{-\log(1-s2^{-s})}.$$

Note that the upper bound for $G_1(r,s)$ improves the lower bound for the rate of s–wise intersecting codes.
In Section 5 we show that hypergraph covering can be used to obtain in a simple way good upper bounds for generic erasure correcting sets, (r,s)–sets, and stopping redundancy of a linear code.

II. Properties of generic (r,s)–sets

Hollmann and Tolhuizen obtained the following characterization of generic (r,s)–sets.

Proposition 1: [17] A subset $\mathcal{A} \subset \mathbb{F}^r$ is generic (r,s)–set if and only if for every full rank matrix $M \in \mathbb{F}^{r\times s}$ there exists $\mathbf{a} \in \mathcal{A}$ such that $wt(\mathbf{a}M) = 1$.

We extend this characterization as follows

Proposition 2: A subset $\mathcal{A} \subset \mathbb{F}^r$ is a generic (r,s)–set if and only if for every full rank matrix $M \in \mathbb{F}^{r\times s}$ the set $\{\mathbf{x} \in \mathbb{F}^s : \mathbf{x} = \mathbf{a}M, \mathbf{a} \in \mathcal{A}\}$ contains a hyperplane not passing through the origin.

Proof: For integers $1 \leq t \leq s < r$ and a set of linearly independent vectors $S = \{\mathbf{v_1}, \ldots, \mathbf{v_t}\} \subset \mathbb{F}^{\mathbf{s}}$, let $\mathcal{A} \subset \mathbb{F}^r$ be a subset satisfying the following property with respect to $\{\mathbf{v_1}, \ldots, \mathbf{v_t}\}$:
(P) For every full rank matrix $M \in \mathbb{F}^{r\times s}$ there exists a vector $\mathbf{a} \in \mathcal{A}$ such that $\mathbf{a}H = \mathbf{v_i}$ for some $i \in [t]$.
We claim then that $\mathcal{A}$ satisfies this property with respect to every linearly independent set of vectors $\{\mathbf{x_1}, \ldots, \mathbf{x_t}\} \subset \mathbb{F}^{\mathbf{s}}$.

Let E and X be the matrices formed by the row vectors $\mathbf{v_1}, \ldots, \mathbf{v_t}$ and $\mathbf{x_1}, \ldots, \mathbf{x_t}$ respectively. To prove the claim, we have to show that given a full rank matrix $M \in \mathbb{F}^{r\times s}$, there exists $\mathbf{a} \in \mathcal{A}$ such that $\mathbf{a}M = \mathbf{x_i}$ for some $i \in [t]$. Let $P \in \mathbb{F}^{s\times s}$ be an invertible matrix such that $PE = X$. Then, in view of the property (P) of $\mathcal{A}$, there exists $\mathbf{a} \in \mathcal{A}$ such that $\mathbf{a}(MP^{-1}) = \mathbf{v_i}$ for some $i \in [t]$ and hence $\mathbf{a}M = \mathbf{v_i}P = \mathbf{x_i}$. Let now $t = s$ and let S be the set of s unit vectors in $\mathbb{F}^s$. Then the claim together with Proposition 1 gives the following analogue of Proposition 1.

Proposition 1^* A set $\mathcal{A} \subset \mathbb{F}^r$ is generic (r,s)–set if and only if for any given set of linearly independent vectors $\{\mathbf{v_1}, \ldots, \mathbf{v_s}\} \subset \mathbb{F}^{\mathbf{s}}$ and every full rank matrix $M \in \mathbb{F}^{r\times s}$ there exists $\mathbf{a} \in \mathcal{A}$ such that $\mathbf{a}M = \mathbf{v_i}$ for some $i \in [s]$.

Note also that for $|S| = t = 1$ we have (r,s)–sets and the claim implies the following condition (shown in [16]): $\mathcal{A} \subset \mathbb{F}^r$ is an (r,s)–set if and only if for every full rank matrix $M \in \mathbb{F}^{r\times s}$ the set $\{\mathbf{x} \in \mathbb{F}^s : \mathbf{x} = \mathbf{a}M, \mathbf{a} \in \mathcal{A}\}$ contains all nonzero vectors. This condition clearly means that $\mathcal{A}$ meets every $(r-s)$–flat.

Let now $\mathcal{A}$ be a generic (r,s)–set and let $M \in \mathbb{F}^{r\times s}$ be a matrix of rank s. Let also $\mathbf{u_1}, \ldots, \mathbf{u_s} \in \mathbb{F}^s$ be such that $\{\mathbf{a}M : \mathbf{a} \in \mathcal{A}\} \cap \{\mathbf{u_1}, \ldots, \mathbf{u_s}\} = \emptyset$. Then Proposition 1^* implies that the dimension dimspan$\{\mathbf{u_1}, \ldots, \mathbf{u_s}\} \leq \mathbf{s-1}$. Thus, $\mathbb{F}^s \backslash \text{span}\{\mathbf{u_1}, \ldots, \mathbf{u_s}\}$ contains a hyperplane not passing through the origin. Suppose now $\mathcal{U} \subset \{\mathbf{a}M : \mathbf{a} \in \mathcal{A}\}$ is an $(s-1)$–flat. Then for every linearly independent vectors $\mathbf{u_1}, \ldots, \mathbf{u_s} \in \mathbb{F}^s$ we have $\{\mathbf{u_1}, \ldots, \mathbf{u_s}\} \cap \mathcal{U} \neq \emptyset$. ■

Let $\mathcal{A} \in \mathbb{F}^r$ be a generic (r,s)–set. Let us represent $\mathcal{A}$ by an $|\mathcal{A}| \times r$ matrix A where the rows are the vectors of $\mathcal{A}$. Let also $N \in \mathbb{F}^{r\times}$ be an invertible matrix. Then we get the following.

Corollary 2: (i) In every set of s columns of AN there is a subset of $s-1$ columns that contains each $(s-1)$–tuple.
(ii) $\mathcal{A}$ hits at least $2^{s-1} \begin{bmatrix} r \\ r-s \end{bmatrix}$ $(r-s)$–flats.
(iii) $|\mathcal{A}| \geq 2^{s-1} + k - s$.

Proof: (i) Note first that the rows of AN also define a generic (r,s)–set. Indeed, in view of Proposition 1, for every full rank matrix $M \subset \mathbb{F}^{r\times s}$ (and hence for NM) the matrix $A(NM) = (AN)M$ contains a row of weight one. Now the statement follows from Proposition 2.
(ii) Proposition 2 implies that if $\mathcal{A} \subset \mathbb{F}^r$ is a generic (r,s)–set, then A hits at least 2^{s-1} cosets of every $(r-s)$–subspace in $\mathbb{F}^r$. This implies the statement.
(iii) Without loss of generality we may assume that A contains r unit vectors. Now the statement follows since there exists $s-1$ columns of A that contain all $(s-1)$ nonzero tuples and $k-s+1$ zero tuples. ■

III. Relation to other problems

In this section we show the relationship between (r,s)–sets and intersecting codes studied in the literature.

Intersecting Codes: A linear $[n,k]_q$ code $\mathcal{C}$ over a field $\mathbb{F}_q$ is called *intersecting* if any two nonzero codewords have a common nonzero coordinate. Intersecting codes have been studied by several authors [20], [25], [7], [9], [8]. A $[n,k]_q$ code $\mathcal{C}$ is called *s-wise intersecting* $(s \geq 2)$

if for any s independent vectors in $\mathcal{C}$ there is a coordinate where all the vectors have a nonzero element.

Problem 1 Given integers $2 \leq s \leq k$, determine $n_q(k,s)$ (in case $q=2$ we write $n(k,s)$), the minimum length n of an s-wise intersecting $[n,k]_q$–code.

Proposition 3: Every (k,s)–set $A \subseteq \mathbb{F}_2^k$ with $|A| = n$ is equivalent to an s-wise intersecting $[n,k]$ code and vice versa. As a consequence we have $G_1(k,s) = n(k,s)$.

Proof: . Let $\mathcal{A} \subseteq \mathbb{F}_2^k$ be a (k,s)–set and let $n = |\mathcal{A}|$. Let us represent $\mathcal{A}$ as an $|\mathcal{A}| \times k$ matrix A where the rows correspond to the vectors $\mathbf{a_1}, \ldots, \mathbf{a_n} \in A$, and denote $G = A^T$. Note that $G \in \mathbb{F}_2^{k\times n}$ and $rank(G) = k$. Let $\mathbf{v_1}, \ldots, \mathbf{v_s} \in {\mathbb{F}_2}^k$ be linearly independent vectors and let $\mathbf{u_1} = \mathbf{v_1}G, \ldots, \mathbf{u_s} = \mathbf{v_s}G$. Clearly $\mathbf{u_1}, \ldots, \mathbf{u_s} \in \mathbb{F}_2^n$ are linearly independent. By the definition of a (k,s)–set, there exists $\mathbf{a_i} \in \mathcal{A}$ such that $(\mathbf{a}, \mathbf{v_j}) = 1$ for $j = 1, \ldots, s$, that is all vectors $\mathbf{u_1}, \ldots, \mathbf{u_s}$ have a one in the i-th coordinate. This clearly means that the $[n,k]$ code with the generator matrix G is an s–wise intersecting code. Similarly we have the inverse implication. ■

Let us give another equivalent formulation for the problem of construction of s–wise intersecting (n,k)–codes, respectively (k,s)–sets, as a covering problem.

Problem 1^* Determine the minimal size $n(k,s)$ of a set of vectors in $\mathbb{F}^k$, called a transversal or a blocking set, that meets every $(k-s)$–dimensional flat.

Consider also the dual version of the problem: Find the minimal number of hyperplanes $\mathcal{H}_1, \ldots, \mathcal{H}_n$, not passing through the origin, such that every $(s-1)$–flat (equivalently every set of s linearly independent vectors in $\mathbb{F}_2^k$) is contained in some $\mathcal{H}_i$.

Remark 1 We note that in case $s=1$ we have a triviality and $n(k,1) = k$. Another trivial case is $s = k$. In this case we clearly have $n(k,k) = 2^k - 1$. It is also easy to see that $n(k,k-1) = 2^k - 2$. The first nontrivial case is $s = 2$.

Remark 2 The notion of a (k,s)–set can be extended to arbitrary spaces $\mathbb{F}_q^k$ in a natural way. However, notice that Proposition 3 is not true for the nonbinary case. Consider an MDS $[n,k,d=n-k+1]_q$–code $\mathcal{C}$. Such a code exists for all $1 \leq k \leq n \leq q+1$ (see [24]). Observe that for $d > \frac{s-1}{s} \cdot n$ (that is $n > s(k-1)$) we have an s–wise intersecting code, but the columns of a generator matrix of $\mathcal{C}$ do not form a (k,s)–set for $s \geq 2$.

It is worth to mention that the problem of finding the minimal size of a set of nonzero vectors in $\mathbb{F}_q^k$ that meets all $(k-s)$–dimensional subspaces is much easier. This problem was solved by Bose and Burton [6].

Theorem 5: [6] Let $\mathcal{A}$ be a set of points of $\mathbb{F}_q^k$ that mits every $(k-s)$–space of $\mathbb{F}_q^k$. Then $|\mathcal{A}| \geq (q^{r+1}-1)/(q-1)$, with equality if and only if $\mathcal{A}$ consists of the points of an $(r+1)$–subspace of $\mathbb{F}_q^k$.

Covering arrays: A $k \times N$ array with entries from an alphabet of size q is called a t-covering array, and denoted by $CA(N,k,t)_q$, if the columns of each $t \times N$ subarray contain each t-tuple at least once as a column. The problem is to minimize N for which there exists a $CA(N,k,t)_q$. Covering arrays were first introduced by Renyi [26]. The case $t = 2$ was solved by Renyi [26] (for even k) and independenty by Katona [19] and Kleitman and Spencer [21] (for arbitrary k). Covering arrays have applications in circuit testing, digital communication, network designs, etc. Construction of optimal covering arrays has been the subject of a lot of research (see a survey [10]).

The following fact follows directly from Proposition 3.

Proposition 4: An $[n,k]$ code $\mathcal{C}$ is s–wise intersecting if and only if every generator matrix of $\mathcal{C}$ (together with the zero column) is an s–covering array.

Let us also mention another extensively studied related notion. A code $\mathcal{C}$ of length n is called (t,u)–*separating*, if for every disjoint pair (U,T) of subsets of $\mathcal{C}$ with $|T| = t$ and $|U| = u$ the following holds: there exists a coordinate i such that for any codeword $(c_1, \ldots, c_n) \in T$ and any codeword $(c'_1, \ldots, c'_n) \in U$, $c_i \neq c'_i$. Separating codes were studied by many authors in connection with practical problems in cryptography, computer science, and search theory. The relationship between intersecting codes and separating codes is studied in [9].

A. Some known results about intersecting codes

We present some known results on intersecting codes which can be used for our problems. Given a vector $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$, the set $I = \{i \in [n] : v_i \neq 0\}$ is called the support of $\mathbf{v}$ and is denoted by $supp(\mathbf{v})$. Given a code $\mathcal{C}$ of length n and $I = \{i_1, \ldots, i_{|I|}\}$, denote by $\mathcal{C}(I)$ the restriction (projection) of the code on the coordinate set I, that is the code obtained by deletion of the coordinates $\bar{I} \triangleq \{1, \ldots, n\} \setminus I$.

Lemma 1: Let $\mathcal{C}$ be an s-wise intersecting $[n,k]$ code and let $\mathbf{v} \in \mathcal{C}$ be a codeword with $wt(\mathbf{v}) = w$ and with $supp(\mathbf{v}) = I$. Then
(i) [9] $\mathcal{C}(I)$ is an $[w,k]$-code. If $\{\mathbf{u_1}, \ldots, \mathbf{u_{k-1}}, \mathbf{v}\}$ is a base of $\mathcal{C}(I)$ then the code $\mathcal{C}^*(I)$ generated by the vectors $\{\mathbf{u_1}, \ldots, \mathbf{u_{k-1}}\}$ is an $(s-1)$–wise intersecting $[w,k-1]$ code.
(ii) $\mathcal{C}(\bar{I})$ is an $(s-1)$–wise intersecting $[n-w,k-1]$ code.

The proof of (i) is easily derived from the definition of an s–wise intersecting code. Note that both (i) and (ii) follow from Proposition 4. (The lemma was also observed in [16] in terms of (r, s)–sets).

The lemma implies simple estimates for the minimum and maximum distances of intersecting codes. It shows that s-wise intersecting codes have strong distance properties which means that in general construction of such optimal codes is a difficult problem. The next two results are used for construction of infinite families of s-wise intersecting binary codes with positive rate.

Theorem 6: (Cohen–Zemor)[8] The punctured, dual of the 2-error-corecting BCH code with parameters $[2^{2s+1} - 2, 4s + 2, 2^{2s} - 2^s - 1]$, is s-wise intersecting.

Lemma 2: [8] Let $\mathcal{C}_1$ be an $[n_1, k_1, d_1]_q$ code with $q = 2^{k_2}$ and $d_1 > n_1(1 - 2^{1-s})$. Let $\mathcal{C}_2$ be an $[n_2, k_2, d_2]$ binary s-wise intersecting code. Then the concatenation $\mathcal{C}_1 \circ \mathcal{C}_2$ is a binary s-wise intersecting $[n_1 n_2, k_1 k_2, d_1 d_2]$ code.

Theorem 7: [8] There is a constructive infinite sequence of s-wise intersecting binary codes with rate arbitrary close to

$$R = \left(2^{1-s} - \frac{1}{2^{2s+1} - 1}\right) \frac{2s + 1}{2^{2s} - 1} = 2^{2-3s}(s + o(s)). \tag{III.1}$$

The result is obtained by concatenating algebraic-geometric $[n, k, d]_q$ codes in Tsfasmann [29] satisfying $d > n(1 - 2^{1-s})$ with $q = 2^{4s+2}$ and with a rate arbitrary close to $2^{1-s} - 1/(\sqrt{q} - 1)$, with $[2^{2s+1} - 2, 4s + 2, 2^{2s} - 2^s - 1]$ code of Theorem 6.

Another approach for constructing intersecting codes is to use *ε-Biased Codes*. A binary linear code of length n is called ε–biased if the weight of every non-zero codeword in C lies in the range $(1/2 - \varepsilon)n \le w \le (1/2 + \varepsilon)n$. Biased codes can be constructed using pseudo-random graphs known as expanders (expander codes).

Theorem 8: (Alon et al.) [5] For any $\varepsilon > 0$, there exists an explicitly specified family of constant-rate binary linear ε–biased codes.

Lemma 3: (Cohen–Lempel) [7] Let d and D denote respectively the minimum and the maximum distance a binary code $\mathcal{C}$. Then $\mathcal{C}$ is s–wise intersecting if $d > D(1 - 2^{1-s})$.

The next statement follows directly from the lemma.

Corollary 3: An ε–biased linear code is s–wise intersecting if $\varepsilon < 1/(2^{s+1} - 2)$.

The following nonconstructive lower bound for the rate of an s–wise intersecting $[n, k]$ code is due to Cohen and Zemor.

Theorem 9: [8] For any given rate $R < R(s)$

$$R(s) = 1 - \frac{1}{s} \log(2^s - 1) \tag{III.2}$$

and $n \to \infty$ there exists an s–wise intersecting $[n, k]$ code of rate R.

Using recursively the upper bound due to McEliece-Rodemich-Rumsey-Welch [24] together with Lemma 1 (i) one can get upper bounds for the rate of s–wise intersecting codes.

Theorem 10: (Cohen et al.) [9] The asymptotic rate of the largest s–wise intersecting code is at most R_s, with $R_2 \approx 0.28,\ R_3 \approx 0.108, R_4 \approx 0.046, R_5 \approx 0.021, R_6 \approx 0.0099$.

For the case $s = 2$, the best known bounds on the minimal length $n(k, 2)$ of an $[n, k]$- intersecting code are as follows

$$c_1(1 + o(1))k < n(k, 2) < c_2 k - 2, \tag{III.3}$$

where $c_1 = 3.53\ldots, c_2 = \frac{2}{2 - \log 3}$.

The lower bound is obtained by Katona an Srivastava [20]. The upper bound is due to Komlós (see [20], [25], [7]). Note that it coincides with the upper bound in Theorem 2 ([16]) for $s = 2$.

IV. Improving bounds for $G(k, s)$ and $F(k, s)$

In this section we derive new bounds for $G(k, s)$ and $F(k, s)$.

Theorem 11: For $2 \le s < k$ we have

$$G_1(k, s) \ge 3 \cdot 2^{s-2}(k - s) + 5 \cdot 2^{s-2} - 2. \tag{IV.1}$$

Proof: To prove this bound we need the following consequence of Lemma 1.

Lemma 4: For an s–wise intersecting $[n, k, d]$ code $\mathcal{C}$ we have

$$n \ge 2 \cdot n(k - 1, s - 1) + D(\mathcal{C}) - d + 1.$$

Proof: Let $\mathbf{v}$ be a codeword of minimal weight d, with the support set I, that is $wt(\mathbf{v}) = |I| = d$, and let G be a generator matrix of $\mathcal{C}(I)$. We may assume that all rows of G except for the first one have a zero in the first coordinate. Hence by Lemma 1 the code $\mathcal{C}^*(I)$ has the support size $d-1$, that is $d \ge n(k-1, s-1)+1$. Lemma 1 implies also that $D(\mathcal{C}) \le n - n(k - 1, s - 1)$, which together with the previous inequality gives the result. ■

Recall that for $s < k$ we have $n(k, s) < 2^k - 1$. Then the lemma in particular implies the inequality $n(k, s) \ge 2n(k - 1, s - 1) + 2$. This follows from the simple observation that there is no a constant weight $[n, k, d]$ code with $n < 2^k - 1$ and hence $D(\mathcal{C}) > d$

(the inequality also follows from the fact that in case $n(k,s) < 2^k - 1$ we have $n \geq 2d$). Since $\mathcal{C}^*(I)$ is an $[d,k,d']$ code, there is a codeword $\mathbf{u} \in \mathcal{C}$ of weight at most d' in the support set I of $\mathbf{v}$. Observe that this implies $2d - 2d' \leq D(\mathcal{C}) \leq n - n(k-1,s-1)$ and hence $n \geq n(k-1,s-1) + 2d - 2d'$, where d' is the minimum weight of $\mathcal{C}(I)$. Note that $d' \leq d - k + 1$ and thus $n \geq n(k-1,s-1) + 2k - 2$. This in particular for $s = 2$ (together with $n(k-1,1) = k-1$) implies that $n(k,2) \geq 3k - 3$. We have now the relation $G_1(k,s) \geq 2G_1(k-1,s-1) + 2$ with $G_1(k,2) = n(k,2) \geq 3k - 3$. Using induction on s we get the required result. ∎

Note that the bound is tight for $s = k-1$. Indeed, for this case we have $G(k,k-1) \geq 3 \cdot 2^{k-3} + 5 \cdot 2^{k-3} - 2 = 2^k - 2$.

On the other hand observe that any set of $2^k - 2$ nonzero vectors is a $(k,k-1)$–set. Note that the corresponding $(k-1)$–wise intersecting set is a punctured simplex code of length $2^k - 2$.

Theorem 12: For $2 \leq s < k$ we have
$G_1(k,s) \leq$

$$\min_{N \in \mathbb{N}} \Big\{ N : \prod_{j=1}^{N} \Big(1 - \frac{2^{k-s}}{2^k - j}\Big)(2^s - 1) \begin{bmatrix} k \\ s \end{bmatrix} < 1 \Big\}. \quad \text{(IV.2)}$$

Proof: Our problem is to find a blocking set of (minimum) size N with respect to the $(k-s)$-dimensional flats in $\mathbb{F}_2^k$. Let U be a $(k-s)$–flat and let $B = \mathbb{F}_2^k \setminus U$. The subset B with $|B| = 2^k - 1 - 2^{k-s}$ does not contain a blocking set. Thus, for every fixed U there are $\binom{2^k - 2^{k-s}}{N}$ bad N–sets (N–sets which are not blocking sets) in B. The number of all $(k-s)$–flats is $(2^s - 1) \begin{bmatrix} k \\ k-s \end{bmatrix}$. Therefore, the number of bad sets of size N is less than $\binom{2^k - 1 - 2^{k-s}}{N-k} (2^s - 1) \begin{bmatrix} k \\ k-s \end{bmatrix}$. If now $\binom{2^k - 1 - 2^{k-s}}{N} (2^s - 1) \begin{bmatrix} k \\ k-s \end{bmatrix} < \binom{2^k - 1}{N}$ (the number of all N–subsets of $\mathbb{F} \setminus \{\mathbf{0}\}$) then there exists a blocking set of size N. The latter inequality is equivalent to the following

$$\prod_{j=1}^{N} \Big(1 - \frac{2^{k-s}}{2^k - j}\Big)(2^s - 1) \begin{bmatrix} k \\ s \end{bmatrix} < 1. \quad \text{(IV.3)}$$

This gives the result. ∎

Note that Theorem 12 improves the upper bound in Theorem 4. A closed form expression derived from (4.2) is as follows.

Corollary 4: For $2 \leq s < k$ we have

$$G_1(k,s) < \frac{(k-s+1)s + 2}{-\log(1 - 2^{-s})}. \quad \text{(IV.4)}$$

Proof: We use the following known estimate for the gaussian coefficients which is not hard to verify: $\begin{bmatrix} n \\ m \end{bmatrix} < 2^{m(n-m)} \prod_{i=1}^{m} \frac{1}{(1-2^{-i})} < 2^{m(n-m)+2}$. The left hand side of (4.3) is less than $\Big(1 - \frac{2^{k-s}}{2^k}\Big)^N 2^{s(k-s+1)+2}$. The latter implies that $N \geq \frac{(k-s+1)+2}{-\log(1-2^{-s})}$, hence the result. ∎

Note also that Theorem 12 improves also the bound in Theorem 9. Indeed, Corollary 4 in terms of the rate of an s–wise intersecting code gives the following

Corollary 4:* For integers $2 \leq s < k$ with $\alpha = \frac{s-2}{k}$, there exists an s–wise intersecting $[n,k]$ code of rate

$$R > \frac{1}{1-\alpha}\Big(1 - \frac{1}{s}\log(2^s - 1)\Big) \quad \text{(IV.5)}$$

(with an improved factor $1/(1-\alpha)$).
Proof: Denote the right hand side of (4.4) by $g(k,s)$. Note now that $-\log(1-2^{-s}) = s(1 - \frac{1}{s}\log(2^s - 1)) = sR(s)$. Therefore, in view of Corollary 4, we have

$$R > \frac{k}{g(k,s)} = \frac{ks}{(k-s+1)s+2} \cdot R(s) \geq$$

$$\frac{k}{k-s+2} \cdot R(s) = \frac{1}{1-\alpha}.$$

∎

Theorem 12 can be improved as follows. We know that (in view of equivalence between (k,s)–sets and s–wise intersecting codes) for any set $E \subset \mathbb{F}^k$ of k linearly independent vectors there exists an optimal (k,s)–good set $A \subset \mathbb{F}^r$ such that $E \subset A$. Thus, without loss of generality we may assume that the set of k unit vectors $E = \{\mathbf{e_1}, \ldots, \mathbf{e_k}\}$ is contained in an optimal (k,s)–good set A. Next we calculate how many $(k-s)$–flats hits E (in fact, every set of k independent vectors hits the same number of flats).

Lemma 5: The number of $(k-s)$–flats which the set $E = \{\mathbf{e_1}, \ldots, \mathbf{e_k}\}$ hits equals

$$\beta(k,s) \triangleq \sum_{i=1}^{k-s+1} (-1)^{i-1} 2^{i(k-s+1-i)} \begin{bmatrix} k-i \\ s-1 \end{bmatrix} \binom{k}{i}. \quad \text{(IV.6)}$$

Proof: . Note that each nonzero vector hits $2^{k-s} \begin{bmatrix} k-1 \\ k-s \end{bmatrix}$ $(k-s)$–flats. Indeed, the number of $(k-s)$–flats containing a given vector $\mathbf{e}$ equals to the number of $(k-s)$–subspace not containing $\mathbf{e}$ which is $\begin{bmatrix} k \\ k-s \end{bmatrix} - \begin{bmatrix} k-s \\ k-s-1 \end{bmatrix}$(the number of $(k-s)$–subspaces containing $\mathbf{e}$) $= 2^{k-1} \begin{bmatrix} k-1 \\ k-s \end{bmatrix}$. Also it is not hard to observe that each i–subset of E hits exactly $2^{i(k-s+1-i)} \begin{bmatrix} k-i \\ s-1 \end{bmatrix}$ common $(k-s)$–flats (we leave the proof to the reader). To get the result we use now the inclusion-exclusion principle. ∎

We can repeat now the arguments in the proof of Theorem 12 with respect to remaining $2^k - k$ vectors to show that the number of bad $(N-k)$–sets is less than

$$\binom{2^k-k-2^{k-s}}{N-k}\Big((2^s-1)\begin{bmatrix}k\\ s\end{bmatrix}-\beta(k,s)\Big). \qquad \text{(IV.7)}$$

Hence, if the latter quantity is less than $\binom{2^k-k}{N-k}$ then there exists a blocking set of size N. Thus, we have the following

Theorem 13: For integers $2 \le s < k$ we have

$$G(k,s) \le \min_{N\in\mathbb{N}}\Big\{N : \prod_{j=0}^{N-k-1}\Big(1-\frac{2^{k-s}}{2^k-k-j}\Big)\times$$

$$\Big((2^s-1)\begin{bmatrix}k\\ s\end{bmatrix}-\beta(k,s)\Big)< 1\Big\}. \qquad \text{(IV.8)}$$

Next we derive bounds for $F(k,s)$. We start with a lower bound. Recall that in view of Corollary 3 we have $F(k,s) \ge 2^{s-1}+k-s$.

Theorem 14: For integers $4 \le s \le k-1$ and $t \in \mathbb{N}$ we have

$$F(k,s) \ge \min_{2\le t\le s}\max\{G(k,t-1),G(k-t,s-t)\}. \qquad \text{(IV.9)}$$

Proof: Let $\mathcal{A} \subset \mathbb{F}^r$ be a generic (k,s)–set with $|\mathcal{A}| = N$ and let $A \in \mathbb{F}^{k\times N}$ be a matrix where the columns are the vectors of $\mathcal{A}$. Let also $\mathcal{C} \subset \mathbb{F}^N$ be the $[N,k]$ code generated by A. Suppose now that t is the smallest number such that there exists a subset $B \subset \mathcal{C}$ of t linearly independent vectors which is not t–wise intersecting. Thus, $\mathcal{C}$ is $(t-1)$–wise intersecting but not t–wise intersecting. Clearly, without loss of generality, we may assume that the rows of A contain the vectors of B. Let us denote by A' the $(k-s)\times N$ submatrix of A obtained after removing all row vectors of B. We claim now that the code $\mathcal{C}'$ generated by A' is an $(s-t)$–wise intersecting $[N,k-t]$ code. Suppose this is not the case, and let $D \subset \mathcal{C}'$ be a set of $s-t$ linearly independent vectors which are not $(s-t)$–wise intersecting. Observe then that the set $B \cup D$ of s independent vectors does not contain an $(s-1)$–wise intersecting subset, a contradiction. This implies that given t, we have $F(k,s) \ge \max\{G(k,t-1),G(k-t,s-t)\}$ and hence the result. ∎

Corollary 5: Given integers $4 \le s \le k-1$ we have

$$F(k,s) \ge G(k-\lceil s/2\rceil,\lfloor s/2\rfloor). \qquad \text{(IV.10)}$$

Proof: We have $G(k-t,s-t) \ge G(k-\lceil s/2\rceil,\lfloor s/2\rfloor)$ for $1 \le t \le \lceil s/2\rceil$. In case $t > \lceil s/2\rceil$ we have $G(k,t-1) > G(k-\lceil s/2\rceil,\lfloor s/2\rfloor)$. This implies that $\min_{2\le t\le s}\max\{G(k,t-1),G(k-t,s-t)\} \ge G(k-\lceil s/2\rceil,\lfloor s/2\rfloor)$. ∎

Note that this improves the lower bound $F(k,s) \ge k$. Using, for example the lower bound (1.6) for $G(k,s)$ we get $F(k,s) \ge G(k-\lceil s/2\rceil,\lfloor s/2\rfloor) \ge 2^{\lfloor \frac{s}{2}\rfloor-1}(k-s+2)$. Thus, we have

$$F(k,s) \ge \max\{2^{s-1}+k-s, 2^{\lfloor \frac{s}{2}\rfloor-1}(k-s+2)\}.$$

In particular, note that for $s = 4$ we get $F(k,4) \ge G(k-2,2) \ge 3(k-3)$.

Theorem 15: For integers $2 \le s < k$ we have

$$F(k,s) \le$$

$$\min_{N\in\mathbb{N}}\Big\{N : \prod_{j=1}^{N}\Big(1-\frac{s2^{k-s}}{2^k-j}\Big)\frac{1}{s!}\prod_{i=0}^{s-1}(2^s-2^i)\begin{bmatrix}k\\ s\end{bmatrix}< 1\Big\}. \qquad \text{(IV.11)}$$

Proof: To each $(k-s)$–subspace $U \subset \mathbb{F}^k$ we put into correspondence a fixed generator matrix $H \in \mathbb{F}^{s\times k}$ of the dual space $V^\perp$, that is $U = \{\mathbf{x} \in \mathbb{F}^k : \mathbf{x}H^T = \mathbf{0}\}$. For example, taking the set of all $s\times r$ matrices of rank s in reduced row echelon form, we get one–one correspondence between these matrices and the set of all $(k-s)$–subspaces of $\mathbb{F}^k$. Now each coset of U denoted by U_b is uniquely defined by the pair $(H,\mathbf{b})$ where $\mathbf{b} \in \mathbb{F}^s$ and $U_b = \{\mathbf{x} \in \mathbb{F}^r : H\mathbf{x}^T = \mathbf{b}^T\}$. We say that the cosets $U_{b_1},\dots,U_{b_t}$ are linearly independent if the vectors $\mathbf{b_1},\dots,\mathbf{b_t}$ are linearly independent. Let $\mathcal{B}(U)$ denote the set of all cosets of U. We look for an N–subset of $\mathbb{F}^k$ which is a generic (k,s)–set.

In view of Corollary 2, a subset $A \in \mathbb{F}^r$ is a generic (k,s)–set iff for each $(k-s)$–subspace U, it contains a vector from every collection of s linearly independent cosets of U. We estimate now the number of bad sets of size N. We remove from $\mathcal{B}(U)$ a set of s independent cosets and denote the union of these cosets by $\mathcal{S}$. Thus, $|\mathcal{S}| = s2^{k-s}$. Then any N–subset of $\mathbb{F}^k \setminus \mathcal{S}$ is a bad set. The same holds with respect to the cosets of every $(k-s)$–subspace. The number of distinct bases in $\mathbb{F}^s$ is $\frac{1}{s!}\prod_{i=0}^{s-1}(2^s-2^i)$. Therefore, the number of all bad N–subsets is less than $\binom{2^k-1-s2^{k-s}}{N}\frac{1}{s!}\prod_{i=0}^{s-1}(2^s-2^i)\begin{bmatrix}k\\ k-s\end{bmatrix}$. If now this number is less than $\binom{2^k-1}{N}$, the number of all N–subsets of $\mathbb{F}^k\setminus\{\mathbf{0}\}$, then there exists a generic (k,s)–set of size N. The latter is equivalent to

$$\prod_{j=1}^{N}\Big(1-\frac{s2^{k-s}}{2^k-j}\Big)\frac{1}{s!}\prod_{i=0}^{s-1}(2^s-2^i)\begin{bmatrix}k\\ s\end{bmatrix}< 1.$$

This implies the result. ∎

A closed form expression derived from (4.10) is as follows.

Corollary 6: For $2 \le s < k$ we have

$$F(k,s) < \frac{sk-\log s!}{-\log(1-\frac{s}{2^s})}. \qquad \text{(IV.12)}$$

Proof: Simple calculations show that the left hand side of (4.13) is less than $(1-\frac{s}{2^s})^N 2^{sk}/s!$. ■

V. Bounds derived by a hypergraph covering

In this section we show, that hypergraph covering can be employed to get good upper bounds for (r,s)–sets, generic erasure correcting sets and stopping redundancy of a linear code. Let $\mathcal{H}=(\mathcal{V},\mathcal{E})$ be a hypergraph with a vertex set $\mathcal{V}$ and an edge set $\mathcal{E}$. Let us denote by $d_{\mathcal{V}}=\min_{v\in\mathcal{V}} deg(v)$ (minimal vertex degree) and by $D_{\mathcal{V}}=\max_{v\in\mathcal{V}} deg(v)$ (maximal vertex degree) of $\mathcal{H}$. Analogously we define the minimal edge degree $d_{\mathcal{E}}$ and the maximal edge degree $D_{\mathcal{E}}$. The following simple lemma was found in 1971 and published in larger contexts in [1] (see also [3]).

Covering Lemma 1: For every hypergraph $(\mathcal{V},\mathcal{E})$ there exists a covering (of the vertices by an edge set) $\mathcal{C}\subset\mathcal{E}$ with

$$|\mathcal{C}|\le\frac{|\mathcal{E}|}{d_{\mathcal{V}}}\log|\mathcal{V}|. \tag{V.1}$$

For most parameters a slightly better result was published in [18],[28], and [23].

Covering Lemma 2: For every hypergraph $(\mathcal{V},\mathcal{E})$ there exists a covering of edges (by a vertex set) $C\subset\mathcal{V}$ with

$$|C|\le\frac{|\mathcal{V}|}{d_{\mathcal{E}}}(1+\ln D_{\mathcal{V}}). \tag{V.2}$$

We apply now these resuts to our problems.

(r,s)–sets or s–wise intersecting codes:

We first apply Covering Lemma 1. Consider the dual version of Problem*. The vertex set is the the set of all $(s-1)$–flats in $\mathbb{F}^r$ and the edge set is the set of all $(r-1)$–flats, that is the set of all hyperplanes not passing through the origin. Recall that the number of all $(s-1)$–flats is $(2^{r-s+1}-1)\begin{bmatrix} r\\ s-1\end{bmatrix}$ Thus, we have a regular uniform hypergraph $(\mathcal{V},\mathcal{E})$ with $|\mathcal{V}|=2^r-1$ and $|\mathcal{E}|=(2^{r-s+1}-1)\begin{bmatrix} r\\ s-1\end{bmatrix}$. Observe that the number of hyperplanes in $\mathcal{E}$ containing a given $(s-1)$–flat is $d_{\mathcal{V}}=2^{r-s}$. In view of the lemma there is a covering $\mathcal{C}$ with

$$|\mathcal{C}|\le\frac{2^r-1}{2^{k-s}}\Big(r-s+1+\log\begin{bmatrix} r\\ s-1\end{bmatrix}\Big)<2^s(r-s+1)s+2).$$

Corollary 7: For integers $2\le s\le r$ we have

$$G_1(r,s)<2^s((r-s+1)s+2). \tag{V.3}$$

Recall that the upper bound in Theorem 4 is approximately $2^s\ln 2(rs-\log s!)$.

Next we apply Covering Lemma 2. The vertex set $\mathcal{V}$ is the set of nonzero vectors in $\mathbb{F}^r$ and the edge set $\mathcal{E}$ is the set of all $(r-s)$–flats. The number of all $(r-s)$–flats is $(2^s-1)\begin{bmatrix} r\\ r-s\end{bmatrix}$. Thus, we have a regular uniform hypergraph whith $|\mathcal{V}|=2^r-1$ and $|\mathcal{E}|=(2^s-1)\begin{bmatrix} r\\ r-s\end{bmatrix}$. Each $(r-s)$–flat has size 2^{r-s}, that is $d_{\mathcal{E}}=2^{r-s}$. The number of $(r-s)$–flats in $\mathbb{F}_2^r$ containing a given vector is $2^{r-s}\begin{bmatrix} r-1\\ s-1\end{bmatrix}$. Thus, the vertex degree is $d_{\mathcal{V}}=2^{r-s}\begin{bmatrix} r-1\\ s-1\end{bmatrix}$. In view of the lemma there is a covering C with

$$|C|\le\frac{2^r-1}{2^{r-s}}\Big(1+\ln\Big(2^{r-s}\begin{bmatrix} r-1\\ s-1\end{bmatrix}\Big)\Big)<$$
$$2^s(1+(r-s)s\ln 2+2\ln 2).$$

Corollary 8: For integers $2\le s\le r$ we have

$$G_1(r,s)<2^s(s(r-s)\ln 2+2\ln 2+1). \tag{V.4}$$

Next we show that there are "good" (r,s)–sets with an interesting structure: a union of s–subspaces of $\mathbb{F}^r$. To this end we need the following simple fact.

Lemma 6: A set of vectors $A\subset\mathbb{F}^r$ is (r,s)–set if for every $(r-s)$–space $V\subset\mathbb{F}^r$ there exists an s–space $U\subset A$ such that $V\cap U=\mathbf{0}$.

Proof: The proof is straightforward. Given an $(r-s)$–space V, the fact that the direct sum $V+U=\mathbb{F}^r$ implies that U hits every coset of V. ■

Consider a bipartite graph $\mathcal{G}=(\mathcal{U}\cup\mathcal{V},\mathcal{E})$ with bipartition $\mathcal{U}\cup\mathcal{V}$. Define $\mathcal{V}$ to be the set of all s–subspaces, and $\mathcal{V}$ to be the set of all $(r-s)$–subspaces of $\mathbb{F}^r$. Thus $|\mathcal{U}|=|\mathcal{W}|=\begin{bmatrix} r\\ s\end{bmatrix}$. For $U\in\mathcal{U}$ and $V\in\mathcal{V}$ we have an edge $(U,V)\in\mathcal{E}$ if and only if $U\cap V=\mathbf{0}$. It is easy to see that given an s–subspace U, the number $(r-s)$–subspaces avoiding U is $2^{s(r-s)}$. Hence, the degree of every vertex in $\mathcal{G}$ is $2^{s(r-s)}$. The problem now is to find a minimal cover $C\subset\mathcal{U}$ of the vertices $\mathcal{V}$. This clearly gives us an (r,s)–set.

Every hypergraph can be represented as a bipartite graph (or an incidence matrix) and vice versa. Given a bipartite graph $\mathcal{G}=(\mathcal{U}\cup\mathcal{V},\mathcal{E})$, let $d_{\mathcal{V}}$ be the minimal degree of $\mathcal{V}$ and let $D_{\mathcal{U}}$ be the maximal degree of $\mathcal{U}$. The bipartite graph version of the Covering Lemma 2 is as follows. There exists a covering $C\subset\mathcal{U}$ of $\mathcal{V}$ with

$$|C|\le\frac{|\mathcal{U}|}{d_{\mathcal{V}}}(1+\ln D_{\mathcal{U}}). \tag{V.5}$$

Applying this to our problem we get

$$|C|\le\frac{\begin{bmatrix} r\\ s\end{bmatrix}}{2^{s(r-s)}}(1+\ln 2^{s(r-s)})<4(1+s(r-s)\ln 2).$$

This yields the following result.

Theorem 16: There exists an (k,s)–set (resp. an s–wise intersecting $[n,k]$ code) consisting (resp. with a generator matrix whose columns consist) of a union of less than $4(s(k-s)\ln 2+1)$ subspaces of dimension s.

Generic erasure corecting sets:

The vertex set $\mathcal{V}$ our hypergraph $(\mathcal{V},\mathcal{E})$ is the set of nonzero vectors in $\mathbb{F}^r$. A subset $E \subset \mathcal{V}$ is an edge in $\mathcal{E}$ if and only if E is a union of s linearly independent cosets (defined in the proof of Theorem 15) of an $(r-s)$–subspace. Thus, the degree of each edge is $s2^{r-s}$. The degree of each vertex is $\begin{bmatrix} r-1 \\ s-1 \end{bmatrix} \prod_{i=1}^{s-1}(2^s-2^i)/(s-1)!$. It is clear that a minimal edge covering C gives an optimal generic (r,s)–set, that is $|C| = F(r,s)$. Applying now Covering Lemma 2 we get

$$F(r,s) = |C| \leq \frac{2^r-1}{s2^{r-s}}\Big(1+\ln \frac{\prod_{i=1}^{s-1}(2^s-2^i)\begin{bmatrix} r-1 \\ s-1 \end{bmatrix}}{(s-1)!}\Big) <$$

$$2^s(r\ln 2 - \ln s).$$

Stopping redundancy of a binary linear code:

Let $\mathcal{C}$ be an $[n,k,d]$ code and $\mathcal{C}^\perp$ be its dual code. Let also $r = n-k$ and $s = d-1$. The vertex set $\mathcal{V}$ of our hypergraph is the set of all nonzero vectors of $\mathcal{C}$. Given a set of coordinates $K \subset [n]$ with $|K| \leq s$, let $\mathcal{C}_K^\perp$ be the set of all vectors in $\mathcal{C}^\perp$ which have weight one in K. Note that $|\mathcal{C}_K^\perp| = |K|2^{r-|K|} \geq s2^{r-s}$. Our edge set is defined as $\mathcal{E} = \{\mathcal{C}_K^\perp : K \subset [n], 1 \leq |K| \leq s\}$ Let $C \subset \mathcal{V}$ a minimum vertex cover of the hypergraph $(\mathcal{V},\mathcal{E})$. It is easy to see that if C is a parity check matrix, that is $span(C) = \mathcal{C}^\perp$, then $\rho(\mathcal{C}) = |C|$. Note that dim span$(C) \geq s$. Therefore, adding at most $r-s$ independent vectors to C we get a parity check matrix. Thus, we have $\rho(\mathcal{C}) \leq |C| + r - s$. Observe now that a vector $\mathbf{u} \in \mathcal{C}^\perp$ of weight $wt(\mathbf{u})$ covers $\alpha(\mathbf{u}) = wt(\mathbf{u})\sum_{i=1}^{s}\binom{n-wt(\mathbf{u})}{i-1}$ edges. Let $t = wt(\mathbf{u})$ be the weight for which $\alpha(\mathbf{u})$ is maximal over all choices of $\mathbf{u} \in \mathcal{C}^\perp$. Thus, $(\mathcal{V},\mathcal{E})$ is a hypergraph with the minimal edge degree $d_{\mathcal{E}} = s2^{r-s}$ and maximal vertex degree $\mathcal{D}_{\mathcal{V}} = t\sum_{i=1}^{s}\binom{n-t}{i-1}$. Therefore, applying the Covering Lemma 2 we get

$$|C| < \frac{2^r-1}{s2^{r-s}}\Big(1+\ln\Big(t\sum_{i=1}^{s}\binom{n-t}{i-1}\Big)\Big) <$$

$$\frac{2^s}{s}\Big(1+\ln\sum_{i=1}^{s}\binom{n}{i}\Big).$$

Corollary 9: For an $[n,k,d]$ code $\mathcal{C}$ with $d \geq 3$ we have

$$\rho(\mathcal{C}) < \frac{2^{d-1}}{d-1}\Big(1+\ln\sum_{i=1}^{d-1}\binom{n}{i}\Big)+n-k-d+1.$$

Notice that although we do not always get the best known constants, however we achieve the same order of magnitude for the upper bounds. Since this simple approach gives almost the results above, it should be followed further by finding better covering results using for example Maximal Code Lemma ([2], p.238) or ideas and methods described in ([4], ch.3).

REFERENCES

[1] R. Ahlswede, Coloring hypergraphs: A new approach to multi-user source coding I, Journ. of Combinatorics, Information and System Sciences, Vol. 4, No. 1, 76-115, 1979.

[2] R. Ahlswede, Coloring hypergraphs: A new approach to multi-user source coding-II, J. Combinatorics, Information, and System Science, vol. 5, no. 3, 220–260, 1980

[3] R. Ahlswede, On set coverings in Cartesian product spaces, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 926-937, 2006.

[4] R. Ahlswede and V. Blinovsky, Lectures on Advances in Combinatorics, Universitext, Springer-Verlag, 2008.

[5] N. Alon, J. Bruck, J. Naor, M. Naor, and R. Roth, Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs, IEEE Trans. Inform. Theory, vol. 38, no. 2, 509–516, 1992.

[6] R.C. Bose and R.C. Burton, A characterization of flat spaces in finite geometry and the uniqueness of the Hamming and the MacDonald codes, J. Combin. Theory 1, 96–104, 1966.

[7] G.D. Cohen and A. Lempel, Linear intersecting codes, Discrete Math. 56, 35–43, 1985.

[8] G.D. Cohen and G. Zemor, Intersecting codes and independent families, IEEE Trans. Inform. Theory 40, vol. 6, 1872–1881, 1994.

[9] G. Cohen, S. Encheva, S. Litsyn, and H. G. Schaathun, Intersecting codes and separating codes, Discrete Appl. Math., vol. 128, no. 1, 75–83, 2003.

[10] C.J. Colbourn, Combinatorial aspects of covering arrays, Le Matematiche (Catania) 58, 121-167, 2004.

[11] C. Di, D. Proietti, I.E. Telatar, T.J. Richardson, and R.L. Urbanke, Finite-length analysis of low-density parity-check codes on the binary erasure channel, IEEE Trans. Inform. Theory vol. 48 , no. 6, 1570–1579, 2002.

[12] T. Etzion, On the stopping redundancy of Reed-Muller codes, IEEE Trans. Inform. Theory, vol. 52, no. 11, 4867–4879, 2006.

[13] J. Han and P. H. Siegel, Improved upper bounds on stopping redundancy, IEEE Trans. Inform. Theory, vol. 53, no. 1, 90–104, 2007.

[14] J. Han, P. H. Siegel, and A. Vardy, Improved probabilistic bounds on stopping redundancy, IEEE Trans. Inform. Theory. vol. 54, no. 4, 1749–1753, 2008.

[15] T. Hehn, O. Milenkovic, S. Lendner, and J. B. Huber, Permutation Decoding and the Stopping Redundancy Hierarchy of Cyclic and Extended Cyclic Codes, IEEE Trans. Inform. Theory, vol. 54, no. 12, 2008

[16] H.D.L. Hollmann and L.M.G.M. Tolhuizen, Generic erasure correcting sets: Bounds and constructions, J. Combin. Theory A 113, 1746–1759, 2006.

[17] H.D.L. Hollmann and L.M.G.M. Tolhuizen, On parity-check collections for iterative erasure decoding that correct all correctable erasure patterns of a given size, IEEE Trans. Inform. Theory, vol. 53, no. 2, 823–828, 2007.

[18] D.S. Johnson, Approximation algorithms for combinatorial problems, J. Comput. System Sciences, vol. 9,256–298, 1974.

[19] G.O.H. Katona, Two applications (for search theory and truth functions) of Sperner type thorems, Periodica Math. Hung 3, 19–26, 1973.

[20] G.O.H. Katona and Srivastava, Minimal 2-coverings of a finite affine space based on $GF(2)$, J. Statist. Plann. Inference 8, no. 3, 375–388, 1983.

[21] D.K. Kleitman and J. Spencer, Families of k–independent sets, Discrete Math 6, 255-262, 1973.

[22] J. Komlós and A. G. Greenberg, An asymptotically fast non-adaptive algorithm for conflict resolution in multiple-access channels, IEEE Trans. Inform. Theory, vol. 31, 302–306, 1985.
[23] L. Lovász, On the ratio of optimal and fractional covers, Discrete Math. 13, 383–390, 1975.
[24] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error Correcting Codes, North Holland Mathematical Library, 1977.
[25] D. Miklos, Linear binary codes with intersecting properties, Discrete Appl. Math. 9, no. 2, 187–196, 1984.
[26] A. Rényi, Foundations of probability, Wiley, New York, 1971.
[27] M. Schwartz and A. Vardy, On the stopping distance and the stopping redundancy of codes, IEEE Trans. Inform. Theory, vol. 52, no. 3, 922–932, 2006.
[28] S.K. Stein, Two combinatorial covering problems, J. Comb. Th. A, vol. 16, 391–397, 1974.
[29] M.A. Tsfasmann, Algebraic-geometric codes and asymptotic problems, Discrete Appl. Math. 33, 241–256, 1991.
[30] J. H.Weber and K. A. Abdel-Ghaffar, Stopping set analysis for Hamming codes, in Proc. IEEE ISOC Information Theory Workshop on Coding and Complexity, Rotorua, New Zealand, Aug./Sep. 2005, 24–24.